

NASA's Independent Verification and Validation (IV&V) Program and Gateway IV&V Project



August 14, 2019

Bill Stanton, Gateway IV&V Deputy Project Manager

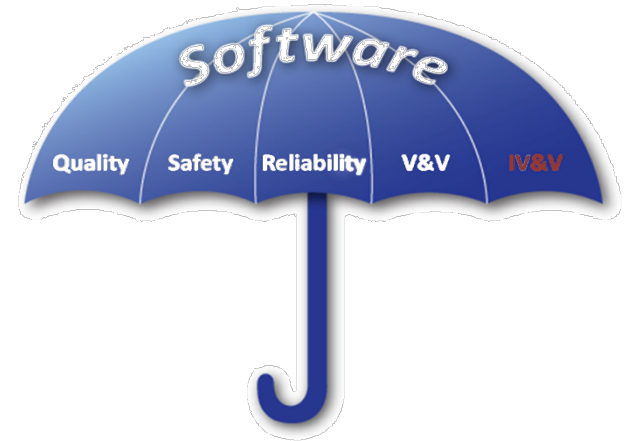
Fairmont, West Virginia

www.nasa.gov/centers/ivv



What is IV&V?

- Verification
 - Are we building the system right?
- Validation
 - Are we building the right system?
- Independent
 - *IEEE Standard for System and Software Verification*, IEEE 1012, defines three important criteria for IV&V independence
 - Technical Independence - Different personnel; not the same people who build it
 - Managerial Independence - Planning and scoping control. Independent reporting path
 - Financial Independence - Funding from a source separate from project development

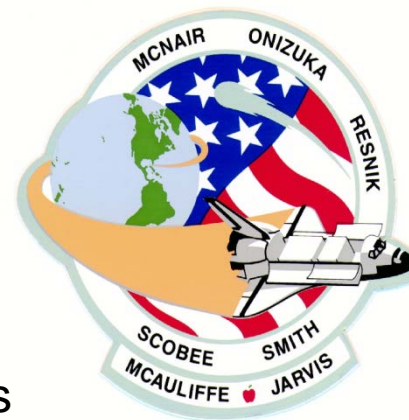




Origins of IV&V within NASA

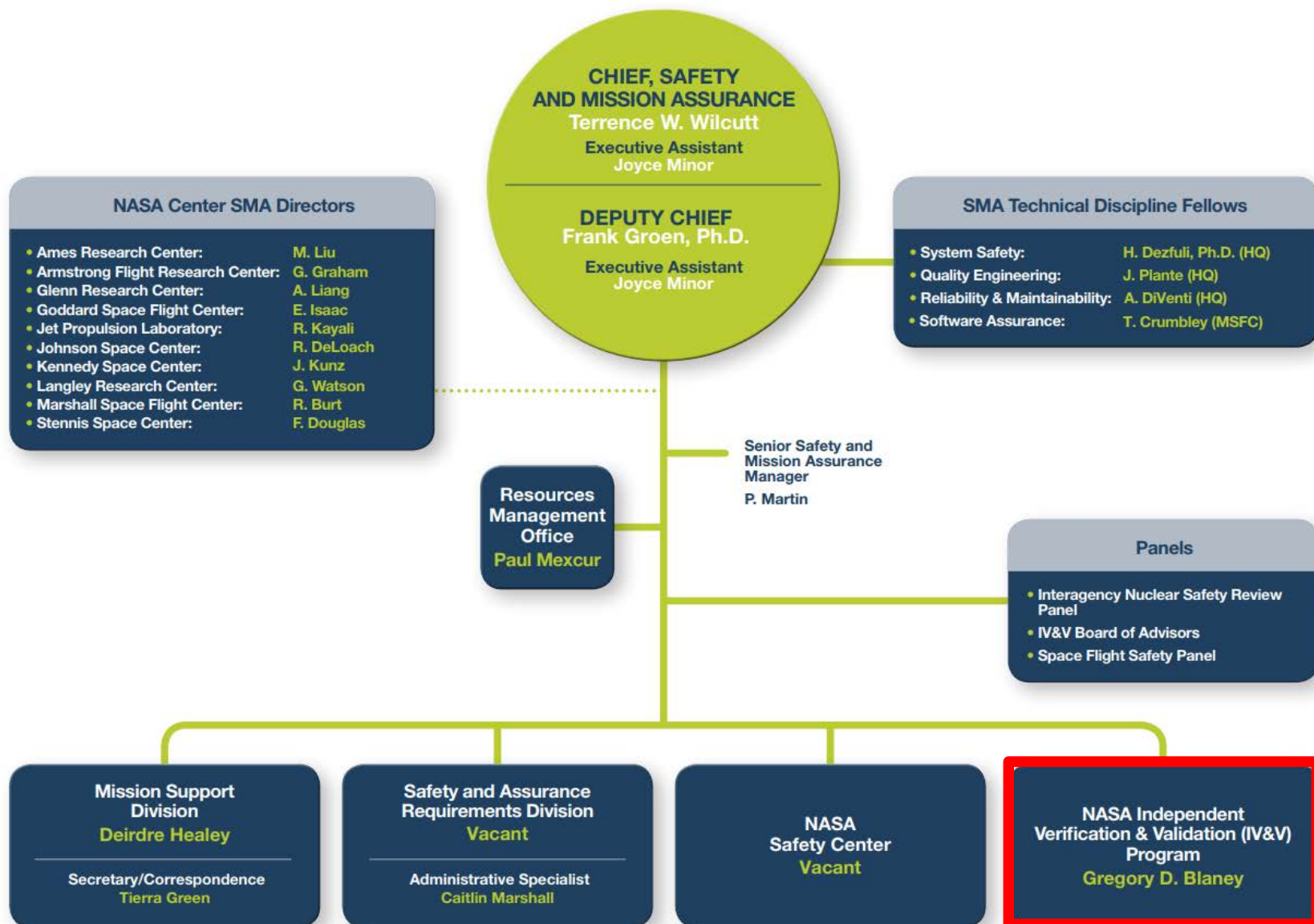


- NASA's IV&V Program: established in 1993
- Founded under the NASA Office of Safety and Mission Assurance (OSMA) as a direct result of recommendations made by the National Research Council (NRC) and the Report of the Presidential Commission on the Space Shuttle Challenger Accident.



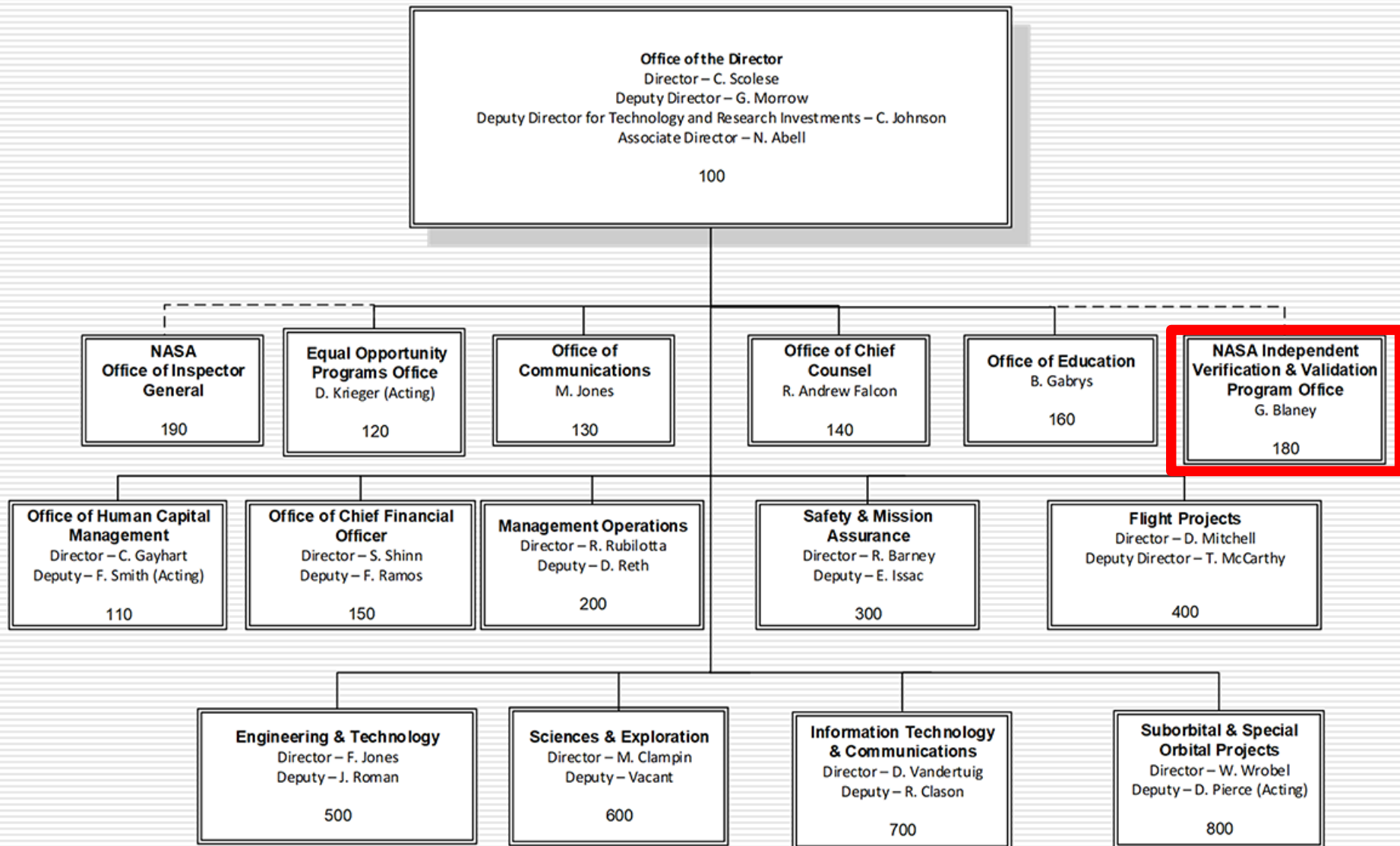


Office of Safety and Mission Assurance



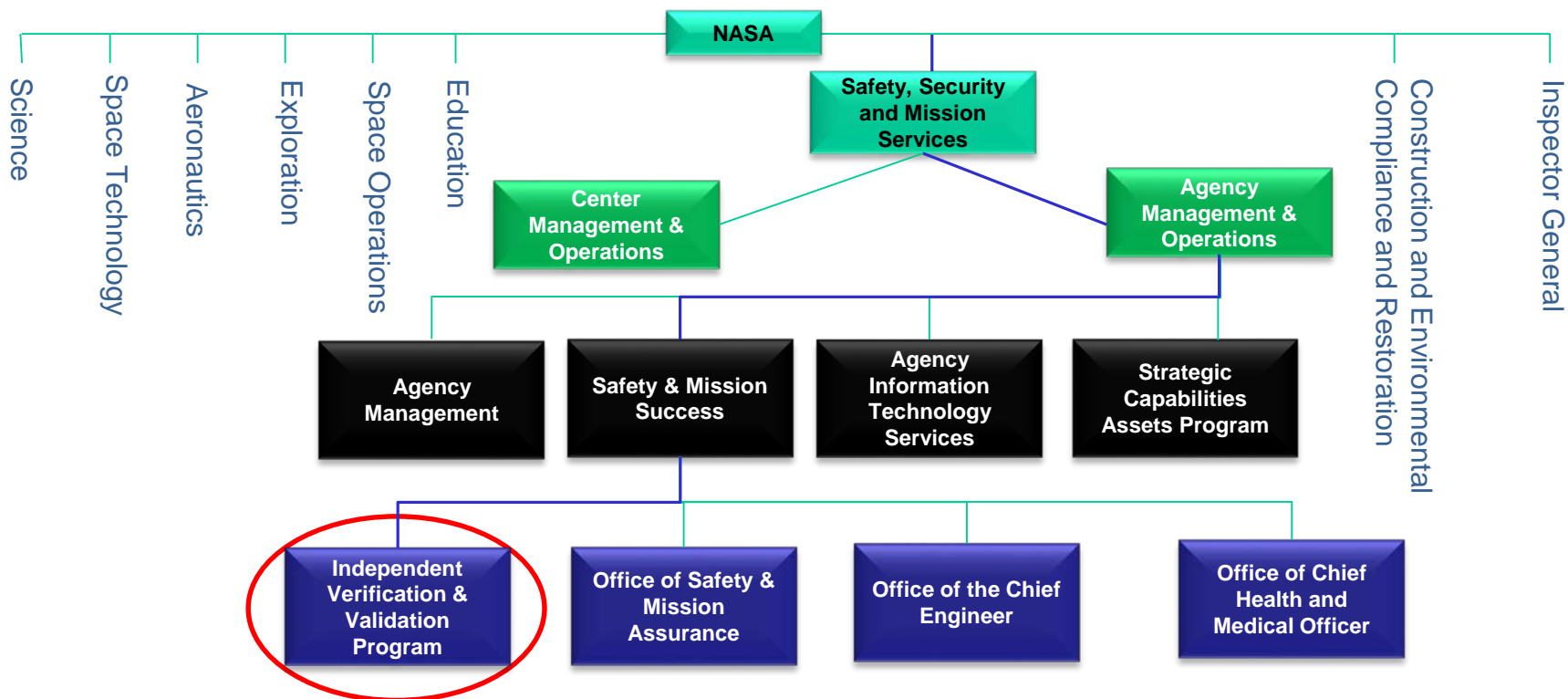


Goddard Space Flight Center - Center Org Chart





Agency Budget Structure



IV&V Program budget covers all IV&V Program needs, including technical work, physical and IT infrastructure, security, etc.



Benefits of IV&V

- **Increased Safety and Dependability** - Greater confidence-delivered products are error free and meet user needs. Many IV&V-identified defects threaten loss of mission or loss of crew if not resolved
- **Reduced Risk** - Increased likelihood high-risk errors are detected early, allowing time for the development team to evolve a comprehensive solution rather than a forced makeshift fix to accommodate deadlines
- **Greater Management Insight** - Increased insight into project status and performance through independent perspective and objective evidence
- **Reduced Cost** - Reduced development rework, reducing total program and project costs for a positive return on investment
- **More Knowledge Transfer** – Increased communication across project teams and cross-project transfer of system and software engineering best practices

IV&V is an industry-proven approach to increase quality, reduce risk, gain development insight, reduce cost, and transfer knowledge



NASA's IV&V Approach

- **Full Lifecycle** - Not just testing at the end. For NASA, IV&V starts near Mission SRR, continues up to, and sometimes beyond, launch
- **Product Focused** – Not document or compliance focused. Examines concept, architecture, requirements, design, code, and test products
- **Capability Based Assurance (CBA)** – Keeping the “big picture” in view when assessing the software details
- **Follow the Risk** – Dynamically adapting plans to focus assurance activities where evidence indicates there is risk
- **Use Multiple Perspectives for Analyses**

Add assurance the software will do what it is supposed to do

Add assurance the software will not do what it is not supposed to do

Add assurance the software will respond appropriately under adverse conditions

NASA IV&V is a systems engineering process employing rigorous methodologies for evaluating the correctness and quality of software products throughout the SDLC for NASA's highest profile missions.



IV&V Assurance Strategy: Concept

- The IV&V Assurance Strategy is the identification/selection of
 - Which mission capability and system software risk to target
 - Which IV&V techniques to use to help reduce the targeted risk
- IV&V techniques include assessments, analyses, evaluations, reviews, inspections, and testing of software artifacts during the entire development lifecycle that create evidence
 - Aligned with IEEE 1012
 - Documented in a Catalog of Methods
- How much evidence? → it is a trade-off between criticality of the system(s) being acquired/deployed
 - Life-sustaining subsystems would warrant an evidence package that clearly & objectively shows the software will operate safely (or clearly shows that it won't)
 - Data management subsystems may warrant less of an evidence package
- The amount and type of evidence needed determines the rigor of the analysis
 - Analytical Rigor is the type and amount of IV&V techniques to use



How IV&V Uses Evidence

- Support recommendations for the developers that improve the quality (or reliability) of the system software
- Support assurance conclusions about the quality (or reliability) of the system software
- Adjust the IV&V Assurance Strategy to focus on the most critical software
- Gain insight into the progress of development
- Evaluate thoroughness of analysis



Establishing an IV&V Assurance Strategy

- The IV&V Program assesses a mission system to determine:
 - The inherent risk associated with the system capabilities
 - The role of software in those capabilities
 - Which software elements of the system warrant IV&V analysis
 - Software elements are generally the focal point of IV&V analyses; however, other lifecycle artifacts (for example: concept documentation, system design, etc...) are utilized to inform lower-level analyses
- The IV&V Program's process for this assessment is called "Portfolio Based Risk Assessment" (PBRA)
 - Results in scores for impact (a measure of the effect of a problem) and likelihood (the potential for the existence of errors) for each system capability and software element
 - Enables informed decision making regarding:
 - What parts of the system should IV&V work on
 - What analytical rigor should IV&V apply (for example: dynamic analysis should be conducted to thoroughly test the implementation of the protocol used for communications)

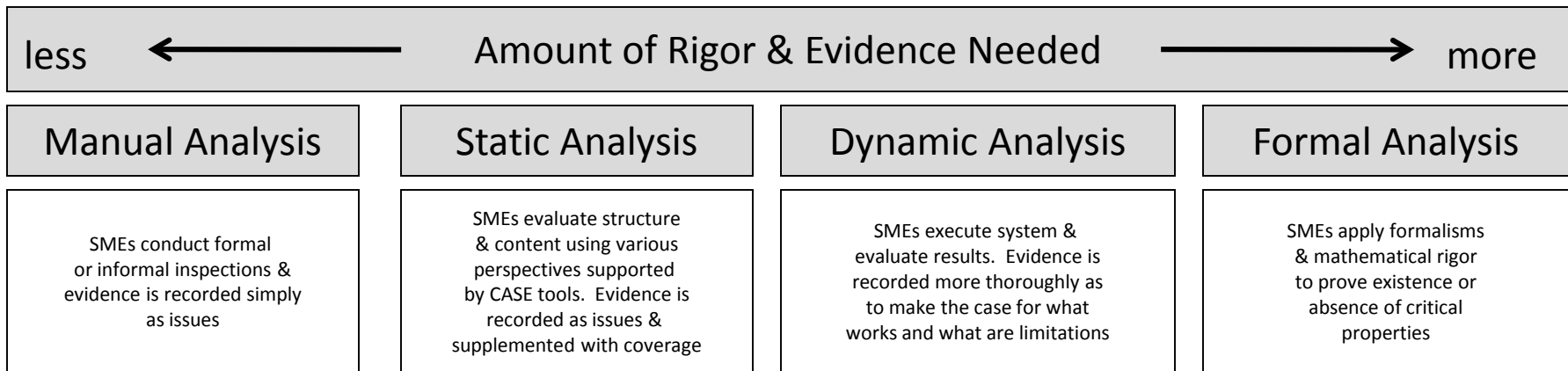


Establishing an IV&V Assurance Strategy (continued)

			Responsible Subsystems						
Desired Capabilities			Cruise - GNC	1 Cruise - Thermal	2 Cruise - Telecom	Cruise Power	3 EDL GNC	Rover: Startup & Initialization	Rover: C&DH
Conduct habitability investigations									
Launch to Mars									
Cruise to Mars			x	x	x	x		x	x
Trajectory control			x		x				
Attitude Control			x		x				
Approach Mars							x		
Trajectory control			x				x		
Attitude Control			x						
Maintain flight systems									
Establish and maintain power						x			x
Establish and maintain thermal control				x					x
Perform fault detection									x
Establish and maintain communications					x			x	x
Gather engineering and housekeeping data			x	x	x	x	x	x	x
EDL									
Pre-EDL							x		
Entry							x		
Descent							x		
Landing							x		
Perform surface operations									
Traverse the Martian surface								x	x
Acquire and handle samples								x	x
Evaluate current position via TRS data									
Perform reconnaissance activity								x	x
Collect science data								x	x

		Subsystem Criticality Profile				
Likelihood	5					
	4				3	
	3		1	2		
	2					
	1					
		1	2	3	4	5
		Impact				

Subsystem 1 – do not recommend IV&V
 Subsystem 2 – recommend IV&V utilizing Static Analysis
 Subsystem 3 – recommend IV&V utilizing Dynamic Analysis
 Subsystem n ...





Implementing an IV&V Assurance Strategy

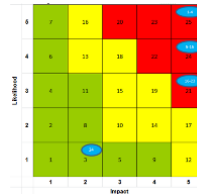
- An IV&V Assurance Strategy is implemented by a set of Analysis Activities
 - Each Analysis Activity achieves one or more IV&V Project's Assurance Objective
 - The IV&V Assurance Strategy informs the Technical Reference and which IV&V technique to use
 - An Analysis Activity generates the evidence for a specific Assurance Objective
- Possible outcomes of implementing the IV&V Assurance Strategy
 - Assurance Conclusions at varying levels of confidence and that that are based on evidence from analyses performed
 - Findings or defects: "Issues", a.k.a "TIM"s (Technical Issue Memorandum)
 - Candidate technical risks for adoption by the Program or Project
 - Refinement of the technical reference
 - Refinement of IV&V Assurance Strategy



IV&V Assurance Strategy

Implementation Process and *Example*

1. Risk-Prioritize System Capabilities and Software for Assurance using PBRA/RBA and IVV S3106, and Develop High-Level Assurance Objectives (AOs)



2. Formulate Risk-Driven Assurance Design in Technical Scope and Rigor (TS&R), and Select and Tailor Analysis Methods using COMPASS and IVV 09-1

Capability: Entry, Descent, and Landing (EDL)

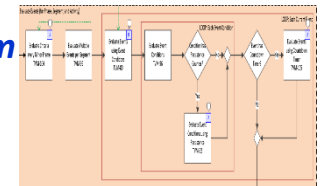
Entity: Orion Timeline Vehicle Manager (TVM)

Objective: *Assure TVM correctly evaluates and detects critical events, to mitigate risk of inappropriate or missed event detection*

Plan: *M-38, Verify Software Design by Inspecting Traces to Requirements (Nominal, Off-Nominal, and Hazard Scenarios)*

3. Develop IV&V Technical Reference, Studying Artifacts and Collaborating with Developers and IV&V Team to Identify IV&V Questions/Concerns to "Follow the Risk"

Learn and Understand: *IV&V created a flow diagram to model condition evaluation and event detection behavior, start to finish, capturing timing, data paths, and interfaces.*



4. **Execute Planned Analysis:** *IV&V traced expectations to TVM software and searched for answers to IV&V Questions/Concerns. IV&V noted differences in comparison logic between code methods intended to provide the same behavior, in critical event condition detection code.*

IV&V Technical Reference

Condition	Equivalent
$ x < y$	$(x < y) \text{ AND NOT } (x \leq -y)$

5. **Confirm Potential Issues:** *IV&V analyzed the logic and proved the code incorrect in 8 separate instances.*

Incorrect Code in Critical Software Method

```

584: case TVM Mission: LESS_THAN:
585:   if ( x <= -y ) {LclRet = false;}
586->: if ( x < y ) {LclRet = true;}
587: break;
  
```

6. **Evaluate Issue Significance and Document Issues:** *The incorrect code would have resulted in incorrect evaluation and detection of critical events, plausibly leading to Loss of Mission (LOM) during EDL, which relies significantly on event-driven behavior (Severity 1).*

7. **Communicate Issue and Track to Resolution:** *Orion accepted and resolved this significant issue.*



IV&V Communication Methods

- Interact with Program and Project staff in working group meetings to establish system understanding and communicate IV&V focus and status
- Communicate findings as soon as possible directly to the developer (e.g. during peer reviews of artifacts or software hosted by the Program, Projects or providers)
- Deliver reports at the completion of major work activities that summarize analysis approaches and results
- Communicate status of assurance objectives and summaries of assurance conclusions in presentations at Program and Project milestone reviews
- Communicate value of IV&V accomplishments in the IV&V Program's weekly reports and monthly status reviews to the Agency



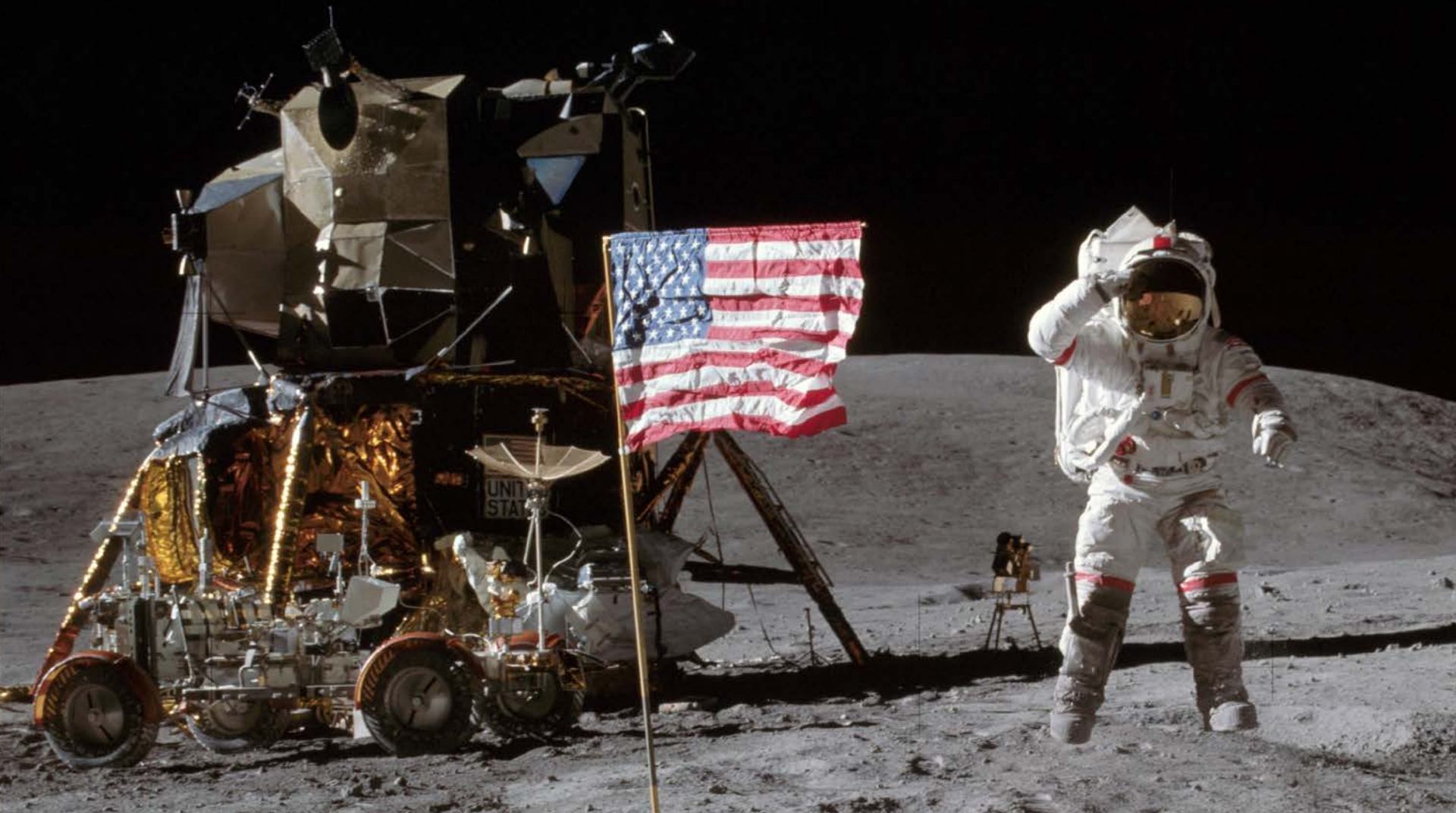
Status of Gateway IV&V

- First round of prioritizing the expected Gateway system capabilities and software and developing high-level Assurance Objectives (AOs) is complete and under internal review within the Program
 - Plan is to review results of the assessment with the Gateway Program and Module Projects
- Finalizing a risk-driven strategy to accomplish the assurance objectives that leverages the IV&V Program's technical framework and applies appropriate analytical rigor
- Developing the IV&V team
- Supporting the Gateway Program's efforts to certify Core Flight Software (CFS) for Gateway



Gateway IV&V Next Steps

- Continue to support CFS certification effort
- Finalize the initial Gateway IV&V Project Execution Plan (IPEP)
 - Identify which Assurance Objectives (AOs) to target and what techniques to use (e.g. exploring option to use formal methods for some AOs like those for assuring autonomous behavior)
 - Review the IPEP with the Gateway Program
- Begin executing according to the IPEP
 - Plan analysis activities that targets integrated Gateway system and software artifacts and Gateway module system and software artifacts as they mature and become available
 - Develop technical references in SysML for analysis activities by studying Gateway artifacts and collaborating with Program and Project staff to identify questions/concerns to target analysis (i.e. “Follow the Risk”)
 - Develop plan for establishing an independent Gateway VSM and software test capability for the Gateway IV&V Project



IV&V's Goal is Mission Success



For More Information

https://www.nasa.gov/centers/ivv/program_flyers.html

NASA's Independent Verification and Validation Program

<https://www.nasa.gov/centers/ivv>

NASA's IV&V Program

<https://www.nasa.gov/centers/ivv>

IV&V Program Services

- System and Software Assurance**
Full lifecycle IV&V and independent assurance quality products, reduced risk, greater insight
- Safety and Mission Assurance**
Support across the agency, in-line with the development and standards development
- Cybersecurity and Information Assurance**
Vulnerability assessment, assessment and security training and security testing (penetration testing)
- Software Development, Testing and Verification**
Support across the agency, in-line with the development and standards development
- Educational Outreach**
Educator workshops, equipment loan program



The IV&V Program is a key element for providing the high level of security, reliability and software assurance for NASA's critical systems.

History of IV&V



The maiden launch of space shuttle Challenger, which carried the first TDRS satellite to orbit, was the first time that NASA's IV&V Program was formally established.

NASA's IV&V Program (2004-2010)

NASA's IV&V Program

<https://www.nasa.gov/centers/ivv>

Within NASA's IV&V Program, the Support Office (SSO) is responsible for engineering services provided and Mission Assurance (OSMA) organizations.

Safety and Mission Assurance

Software Hazard Analysis
The SSO performs analysis of safety hazards that controls, mitigates and contributes to the overall system safety. It performs SWHA in parallel or in conjunction with other analysis. This parallel effort could include both hardware and software faults, as well as human factors.

Software Assurance Plan Development
The SSO supports the development of the Software Assurance Plan (SWAP) which delineates the software assurance maintenance required throughout the safety and quality. The primary focus is to formalize and approved by the program manager.

Standards Development and Evaluation
The SSO also supports the following:

- Develops, updates and reviews standards to facilitate the development and testing of software.
- Aids in the development and update of software.
- Performs analysis of Data Requirements necessary information and artifacts programmatically and/or contract IV&V services.
- Reviews the required project documents, NASA-STD-8739.8, NASA's Software Assurance plan, products and release management plan and comply with associated contract(s).
- Manages OSMA's Software Assurance

NASA's IV&V Program (2004-2010)



NASA's IV&V Program

<https://www.nasa.gov/centers/ivv>

With our growing reliance on information system attacks can include a damaged IV&V Program provides cybersecurity services to municipal governments and other interested parties.

IV&V Program Cybersecurity

Vulnerability Assessment Program
NASA's IV&V Program has a skilled team of vulnerability assessors who perform vulnerability assessments of software and supporting infrastructure. They interfaces/firewalls and computer network of Assessment and Authorization (A&A). NASA's IV&V Program is able to accurately assess the security posture of a system's information security management act (ISMA) reviews, as well as manual and automated assessment on NASA and non-NASA system.

Risk Assessment
NASA's IV&V Program applies its years of experience on the right findings. Risk levels are placed on the right findings. Risk levels are placed on the right findings. Risk levels are placed on the right findings.

FedRAMP 3PAO Services
NASA's IV&V Program is accredited to perform Organization (OPAO) under the Federal Risk (www.fedramp.gov). FedRAMP is a government security assessment, authorization and continuous monitoring program.

Security Training
NASA's IV&V Program has developed a hands-on training for NASA's IV&V Program. The training is designed to enhance the understanding of security concepts and procedures. The training is designed to enhance the understanding of security concepts and procedures.

Security Testing
NASA's IV&V Program offers a variety of representation of a system's assurance level. The testing is designed to enhance the understanding of security concepts and procedures.

NASA's IV&V Program (2004-2010)



NASA's IV&V Program

<https://www.nasa.gov/centers/ivv>

NASA's IV&V Program provides full lifecycle independent assessments for NASA's high priority products, reduced risk, greater insight, reduced customer surveys, and customer quotes of value.

What is IV&V?

Verification answers the question, "Are we building the product right?" It is the process of determining whether or not the software product fulfills the established requirements.

Validation evaluates the software products to ensure that they meet the customer's needs. Validation answers the question, "Are we building the right product?"

Independence in IV&V has three parameters: technical, financial and organizational.

IV&V Benefits

- Higher confidence that delivered products meet requirements.
- An increased likelihood of uncovering defects.
- Delivery of ongoing status indicators and (e.g. program managers).
- Reduction of the need for rework from the start to the end of the project.
- Facilitation of the transfer of system and software knowledge.

Current & Past IV&V Projects

- Commercial Crew Program (CCP)
- Europa
- Ground Systems Development and Operations (GSDO)
- Hubble Space Telescope
- Ice, Cloud, and Land Evaluation Satellite-2 (ICESat-2)
- International Space Station (ISS)

NASA's IV&V Program - 100 University Drive - Fairmont, WV 26554 (304) 367-4200

NASA's Independent Verification and Validation Program EDUCATION OUTREACH

<https://www.nasa.gov/centers/ivv>



Ensuring Safe, Reliable, Secure Operation of Safety & Mission Critical Software

The NASA IV&V Program's education outreach activities inspire and engage West Virginia's youth and have a positive impact on the number of students who choose to pursue careers within.

NASA's IV&V Program

<https://www.nasa.gov/centers/ivv>

SOFTWARE DEVELOPMENT, TESTING & RESEARCH
<https://www.nasa.gov/centers/ivv/jstar/jstar.html>

Within NASA's IV&V Program, the Jon McBride Testing and Research Center (JTC) provides the testing and research services to verify and validate the software products of NASA flight projects. Research and development is done in simulations of embedded system components and space environments.

JSTAR Capabilities

Independent Testing
Independent testing provides the IV&V Program with the ability to dynamically test software. The goal of independent testing is to ensure that must-happen adverse conditions. The independent testing is focused and risk-driven. In such as test scripts and test results as to exactly how the software operates typically performed by IV&V teams on software-only test environments to address the software during testing. Examples of IV&V tests include, but are not limited to, error handling.

Simulation
Within the IV&V Program, the JSTAR team creates software-only environments using hardware emulation, simulation integration, as well as custom in-house simulation software.

Hardware Emulation
This technique provides a means to model physical hardware components, such as flight computers and complex electronic devices (field-programmable gate array, application-specific integrated circuit, etc.) such that the actual flight software can be exercised on an emulated platform. Basically, it enables flight software to be executed on a standard, personal computer versus its intended hardware environment.

Simulation Integration
JSTAR integrates both internally-developed simulation components together, but also integrates simulation components developed by external development organizations (e.g. dynamic simulators, payload simulators, etc.) to create an all-digital spacecraft environment (a single, integrated product).

In-house Simulation Software
Over time, JSTAR has developed a suite of simulation software utilities and tools to make the process of developing simulations of NASA mission systems easier. A few examples of these tools are:

- NASA Operational Simulation (NOS) Engine, passing simulation software to interface two or more simulated components. NOS Engine supports common communications, such as SpaceWire, 1553, 12C and SPI.
- NOS is a software framework that enables software development and V&V of small satellite missions.

The final product of all of this is a JSTAR-developed, software-only simulator, equipping NASA's IV&V Program with the ability to independently test, verify and validate mission elements as well as entire missions without the use of hardware - saving time, money, resources and increasing safety for NASA.

Software Automation
Software Automation enables faster simulation environment deployments and a lightweight means to configuration-manage the test environments. Software automation is the automation of a task in order to test the outcome and behaviors of certain systems and modules. JSTAR utilizes this service to support unit-level testing of in-house developed software, generate virtual machine deployments of in-house developed simulation and test environments, and support testing of customer software. Software Automation is an extremely useful service, and has been provided by JSTAR for many missions and projects to date.



QUESTIONS?





IV&V Program Services

The IV&V Program's mission is to provide our customers assurance that their safety and mission-critical software will operate reliably and safely.

- System and Software Assurance
 - Full Lifecycle IV&V
 - Independent Assessments
- Safety and Mission Assurance (SMA) Support
 - Common support infrastructure for assuring core Software Assurance functions across the Agency
 - Software Assurance Research Program (SARP)
- Mission Protection Services (MPS)
 - Cybersecurity Threat/Risk Assessment, Vulnerability Assessment, Information Assurance (IA) Support, CyberLab, FedRAMP
- Jon McBride Software Testing And Research (JSTAR) Laboratory
 - Independent Test Capability (ITC), Robotics
 - Simulation, Testing, Automation, and Virtualization
- Partnerships, Collaboration, and Leadership
 - MDA, International IV&V WG, WVANG, DOE, OSMA, FBI, NOAA, DOD/Army, CCSDS, OCIO, OCE, STF-1, GSFC Code 300, 400, 500, 700, 800
- STEM Engagement



NASA IV&V Project Metrics

How do IV&V Projects provide the most value to the Agency?

... by getting involved early in the SW development lifecycle

13 of 13 active IV&V projects started before mission SRR.

... by detecting defects in-phase with SW development

Overall phase containment by active projects: **92%** over the past year.

... by detecting and submitting quality defects to the development teams

Overall issue acceptance for active projects was **95%** over the past year.

... by ensuring our customers are satisfied with our products and services

ACTUAL: 2018 Annual Survey: **99.7%** of all responses indicated a favorable (“Agree” or “Strongly Agree”) perception of the support being provided by the IV&V Program.